



Text Part Number: 78-5322-09, Rev. B0

Release Notes for the Cisco 2500 Series Routers for Cisco IOS Release 11.3(11)NA

May 29, 2000

These release notes describe the new features and significant software components for Cisco IOS Release 11.3(11)NA for Cisco 2500 series routers and access servers. The software for Cisco IOS Release 11.3(11)NA is a specialized image designed to support Multimedia Conference Manager features (Gatekeeper and Proxy conforming to H.323). These features must be enabled before running Release 11.3(11)NA software. The Multimedia Conference Manager is briefly described in the section “New Software Features in Release 11.3(2)NA;” for more information, see the Multimedia Conference Manager feature module documentation.



Caution Do not use a router running Release 11.3 NA software as a regular Cisco 2500 router or access server. Routers with Release 11.3 NA installed are designed to be used as dedicated routers for their specialized features only. For example, the Multimedia Conference Manager features can consume significant amounts of CPU processing time when a H.323 call is being established through a proxy; the impact of call establishment on routing performance is not fully determined.

This software release was derived from Cisco IOS Releases 11.3(2)T through 11.3(11)T. For more detailed information about the features and caveats that apply these releases, refer to the *Release Notes for Cisco IOS Release 11.3 T*. Refer also to the *Caveats for Cisco IOS Release 11.3 T* document located on CCO and on the Documentation CD-ROM. For a list of software caveats that apply to Release 11.3(11)NA, refer to the “Caveats” section on page 16 of this document.

Contents

These release notes discuss the following topics:

- System Requirements, page 2
- New and Changed Information, page 4
- Limitations for Release 11.3 NA, page 7
- Important Notes, page 7

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Copyright © 1999
Cisco Systems, Inc.
All rights reserved.

- Caveats, page 16
- Related Documentation, page 21
- Cisco Connection Online, page 24
- Documentation CD-ROM, page 25

System Requirements

This section describes the system requirements for Release 11.3(11)NA and includes the following sections:

- Memory Requirements, page 2
- Cisco 2500 Series Routers and Access Servers, page 2
- Determining Your Cisco IOS Software Release, page 2
- Feature Set List, page 3

Memory Requirements

For Cisco routers to take advantage of the features in the Release 11.3(11)NA IP feature set on Cisco 2500 routers, you must upgrade the code or main system memory as follows:

- Minimum required code memory: 8-MB Flash
- Required main memory: 16-MB DRAM

Some platforms have specific chip or architecture requirements that affect what can be upgraded and in what increments. The Cisco IOS Release 11.3(11)NA IP feature set runs from Flash memory. The image name is c2500-ix-l.

Note Beginning with Cisco IOS Release 10.3, some software image sizes exceed 4 MB and, when compressed, exceed 2 MB. Also, some systems now require more than 1 MB of main system memory for data structure tables.

For Cisco IOS Release 11.3 T memory requirements on Cisco 2500 routers, see the *Release Notes for the Cisco 2500 Series Routers for Cisco IOS Release 11.3 T*. To access this document, see the section “Related Documentation.”

Cisco 2500 Series Routers and Access Servers

For more information on the Cisco 2500 series routers, access servers, and interfaces supported by Release 11.3(11)NA, see the *Release Notes for Cisco IOS Release 11.3 T*.

Determining Your Cisco IOS Software Release

To view the version of Cisco IOS software that is running on your Cisco 2500 series router or access server, log in to the router, and enter the **show version** user EXEC command:

```
router# show version
```

Output from the command is displayed in the second line, as follows:

```
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IX-L), Version 11.3(11)NA RELEASE SOFTWARE
```

Additional command output lines include more information, such as processor revision numbers, memory amounts, hardware IDs, and partition information.

Upgrading to a New Software Release

For information about upgrading to a new software release, refer to the *Cisco IOS Software Release 11.3 Upgrade Paths and Packaging Simplification* product bulletin located on CCO.

From CCO, click **Login** and enter your user ID and password, and then follow this path:

Service & Support: Product Bulletins: Software

Under **Cisco IOS 11.3**, click **Cisco IOS Software Release 11.3 Upgrade Paths (#703: 12/97)**

This product bulletin does not contain information specific to Cisco IOS Release 11.3 NA, but provides generic upgrade information that might apply to Cisco IOS Release 11.3 NA.

Feature Set List

The Cisco IOS software is packaged into “feature sets” (also called “software images”). Each feature set contains a specific subset of Cisco IOS features. Cisco IOS Releases 11.3(2)NA through 11.3(11)NA for Cisco 2500 series routers have one feature set: the IP feature set, containing the Multimedia Conference Manager image.

The following list summarizes the features you can use when running Cisco IOS Release 11.3(11)NA on Cisco 2500 series routers:

- IP Routing:
 - Easy IP (Phase 1)
 - IP Enhanced IGRP Route Authentication
 - TCP Enhancements, including: TCP Selective Acknowledgment and TCP Timestamp
- Management:
 - Cisco Call History MIB Command Line Interface
 - Cisco IOS Internationalization
 - Entity MIB, Phase 1
 - SNMPv2C
 - Virtual Profiles
- Multimedia:
 - H-323 Gatekeeper & Proxy
 - IP Multicast Load Splitting Across Equal-Cost Paths
 - IP Multicast over Token Ring LANs
 - PIM Version 2
 - Stub IP Multicast Routing
- Quality of Service: RTP Header Compression

- Security:
 - Double Authentication
 - HTTP Security
 - Per-User Configuration
 - Reflexive Access Lists
 - Vendor-Proprietary RADIUS Attributes
- Switching: Fast-Switched Policy Routing
- WAN Optimization: PAD Subaddressing
- WAN Services:
 - Bandwidth Allocation Control Protocol
 - Dialer Watch
 - Enhanced Local Management Interface (ELMI)
 - Frame Relay Enhancements
 - Frame Relay MIB Extensions
 - Frame Relay Router ForeSight
 - ISDN Advice of Charge
 - ISDN Caller ID Callback
 - MS Callback
 - Telnet Extensions for Dialout
 - X.25 Enhancements
 - X.25 on ISDN
 - X.25 Switching between PVCs and SVCs
 - X.28 Emulation

New and Changed Information

The following sections list the new features supported by the Cisco 2500 series routers in Cisco IOS Release 11.3 NA.

New Software Features in Release 11.3(11)NA

Release 11.3(11)NA has no new features; however, it supports the features contained in Release 11.3(10)NA. This release also supports features contained in Cisco IOS Release 11.3(11)T, which are described in the *Release Notes for Cisco IOS Release 11.3 T*. To access this document, see the section, “Related Documentation.”

New Software Features in Release 11.3(10)NA

Release 11.3(10)NA has no new features; however, it supports the features contained in Release 11.3(9)NA. This release also supports features contained in Cisco IOS Release 11.3(10)T, which are described in the *Release Notes for Cisco IOS Release 11.3 T*. To access this document, see the section, “Related Documentation.”

New Software Features in Release 11.3(9)NA

Release 11.3(9)NA has no new features; however, it supports the features contained in Release 11.3(8)NA. This release also supports features contained in Cisco IOS Release 11.3(9)T, which are described in the *Release Notes for Cisco IOS Release 11.3 T*. To access this document, see the section, “Related Documentation.”

New Software Features in Release 11.3(8)NA

Release 11.3(8)NA has no new features; however, it supports the features contained in Release 11.3(7)NA. This release also supports features contained in Cisco IOS Release 11.3(8)T, which are described in the *Release Notes for Cisco IOS Release 11.3 T*. To access this document, see the section, “Related Documentation.”

New Software Features in Release 11.3(7)NA

Release 11.3(7)NA has no new features; however, it supports the features contained in Release 11.3(6)NA. This release also supports features contained in Cisco IOS Release 11.3(7)T, which are described in the *Release Notes for Cisco IOS Release 11.3 T*. To access this document, see the section, “Related Documentation.”

New Software Features in Release 11.3(5)NA

Release 11.3(5)NA has no new features; however, it supports the features contained in Release 11.3(4)NA. This release also supports features contained in Cisco IOS Release 11.3(5)T, which are described in the *Release Notes for Cisco IOS Release 11.3 T*. To access this document, see the section, “Related Documentation.”

New Software Features in Release 11.3(4)NA

Release 11.3(4)NA has no new features; however, it supports the features contained in Release 11.3(2)NA with the changes described in this section. This release also supports features contained in Cisco IOS Release 11.3(4)T, which are described in the *Release Notes for Cisco IOS Release 11.3 T*. To access this document, see the section, “Related Documentation.”

The following Multimedia Conference Manager test commands have been removed from Release 11.3(4):

- **test proxy h323 statistics packets**
- **test proxy h323 statistics start**
- **test proxy h323 statistics stop**

The debug command **debug proxy h323 statistics** has been added to the Multimedia Conference Manager feature. You can use this command to enable proxy RTP statistics. The command has no arguments or keywords. To display proxy RTP statistics, enter the command **show proxy h323 detail-call**. To disable the display of proxy RTP statistics, enter the command **no debug proxy h323 statistics**.

New Software Features in Release 11.3(2)NA

This section describes new software features available only in Release 11.3(2)NA and later. For more information about configuring these features, see the new-features documentation online. To access this documentation, see the section “Related Documentation.”

Note Existing Release 11.3(2)T features for Cisco 2500 series routers are supported in Cisco IOS Release 11.3(2)NA. See the *Release Notes for the Cisco 2500 Series Routers for Cisco IOS Release 11.3 T*. To access this document, see the section, “Related Documentation.”

Multimedia Conference Manager

The Cisco Systems Multimedia Conference Manager provides network administrators with a mechanism to support H.323 applications without impacting mission-critical applications. Multimedia Conference Manager also provides the mechanism to implement security for H.323 communications.

H.323 Multimedia Conference Manager, implemented on Cisco IOS software, provides the network administrator with the ability to

- Identify H.323 traffic and apply appropriate policies.
- Limit the H.323 traffic on the LAN/WAN.
- Provide user accounting with records based on the service utilization.
- Inject Quality of Service (QoS) for the H.323 traffic generated by applications such as voice over IP (VoIP), Data conferencing, and video conferencing.

H.323 Proxy

The H.323 Proxy is a boundary device that terminates all H.323 calls from the local LAN or zone and establishes sessions with H.323 endpoints that are in different LANs or zones. Using the Proxy, network administrators can set and enforce QoS policies on WAN segments and provide a method to tag H.323 traffic for tunneling through firewalls.

H.323 Gatekeeper

The H.323 Gatekeeper is an infrastructure component defined by the ITU H.323 standard. This feature provides call routing functionality for H.323 endpoints, provides simple bandwidth management for H.323, and adds authentication, authorization, and accounting functionality for H.323 calls.

Limitations for Release 11.3 NA

The following limitations apply to Release 11.3 NA software.

One Gateway Per Zone

The current Cisco gatekeeper supports only one gateway per zone. More than one gateway can register per zone; however, calls are not forwarded to more than one gateway.

One Proxy Per Zone

The current Cisco gatekeeper supports only one H.323 proxy per zone. More than one proxy can register per zone; however, calls are not forwarded to more than one proxy.

One Local-Zone Declaration

The current Cisco gatekeeper supports only one local-zone declaration. Declarations of more than one local zone in the Cisco gatekeeper are flagged as errors.

No Voice Gateways

The current Cisco gatekeeper supports only H.320 gateways. Voice gateways are not supported. Although voice gateways can register, calls are not forwarded to them.

SNMP Support for Multimedia Conference Manager

SNMP support for Multimedia Conference Manager is not available in Release 11.3(11)NA.

Important Notes

The following sections contain important notes about Cisco IOS Release 11.3 NA that apply to Cisco 2500 series routers. It discusses the following topics:

- Release 11.3 NA on a Cisco 2500 Router
- Legal Regulations
- ATM Multipoint Signaling
- End of Sales and End of Engineering
- Image Deferral, Cisco IOS Release 11.3(8)T
- Enabling IPX Routing
- Forwarding of Locally Sourced AppleTalk Packets
- Missing Source-Route Bridging Commands
- How to Recommend Updates or Changes to the Boilerplate
- New TACACS+ Attribute-Value Pair
- 40-bit Encryption Images are Unavailable in Release 11.3(1)

- Cisco IOS Syslog Failure
- Deprecated MIBs

Release 11.3 NA on a Cisco 2500 Router

Cisco IOS Release 11.3 NA supports Multimedia Conference Manager features (Gatekeeper and Proxy conforming to H.323). Be sure to enable the Multimedia Conference Manager features on Cisco 2500 series routers running this software release. Cisco 2500 routers with Cisco IOS Release 11.3 NA installed are not designed to perform as standard Cisco 2500 series routers or access servers.

The Gatekeeper-to-Gatekeeper Redundancy and Load-Sharing Mechanism feature expands the capability provided by the Redundant H.323 Zone Support feature. Location requests (LRQs) for the Redundant H.323 Zone Support feature are sent simultaneously (in a broadcast fashion) to all of the gatekeepers in the list. The gateway registers with the first gatekeeper that responds and if that gatekeeper becomes unavailable, the gateway registers with another gatekeeper from the list.

The Gatekeeper-to-Gatekeeper Redundancy and Load-Sharing Mechanism feature enhances this capability by allowing you to choose whether the LRQs are sent simultaneously or sequentially (one-at-a-time) to the remote gatekeepers in the list. If the LRQs are sent sequentially, a delay is inserted between the first LRQ and following LRQ. This delay allows the first gatekeeper to respond before the LRQ is sent to the next gatekeeper. The order in which LRQs are sent to the gatekeepers is based on the order in which the gatekeepers are listed (using either the zone prefix or the command **gw-type-prefix**).

Legal Regulations

Cisco IOS images with strong encryption (including, but not limited to 56-bit DES) are subject to U.S. government export controls and have a limited distribution. Images to be installed outside the U.S. require an export license. Customer orders might be denied or subject to delay due to U.S. government regulations. Contact your sales representative or distributor for more information, or send e-mail to export@cisco.com.

In certain countries, use of these products or provision of voice telephony over the Internet might be prohibited and/or subject to laws, regulations or licenses, including requirements applicable to the use of the products under telecommunications and other laws and regulations; customers must comply with all such applicable laws in the country(ies) where they intend to use the products.

ATM Multipoint Signaling

Prior to Cisco IOS Release 11.1(13) and 11.2(8), the command **atm multipoint-signaling** was used on the main interface and affected all subinterfaces. For Release 11.1(13), 11.2(8), and later releases (including Release 11.3), an explicit configuration on each subinterface is required to obtain the same functionality. See caveat CSCdj20944, which is described as follows:

The **atm multipoint-signaling** interface command is currently only available on the main ATM interface. The effect is that signaling behavior (point-to-point or point-to-multipoint) for all clients on all subinterfaces is determined by the command on the main interface. Clients on different subinterfaces can have different behavior. Specifically, 1577 requires point-to-point, and PIM allows point-to-multipoint. The command should be on a per-subinterface basis.

Enable the **atm multipoint-signaling** command on all subinterfaces that require it. Previously, you only needed to enable the command on the main interface.

End of Sales and End of Engineering

End of Engineering (EOE) means there are no more regularly scheduled software maintenance releases. The last maintenance release EOE schedule is available through CCO and Field Service Operations only.

Details are provided in the *End of Sales and End of Engineering for Cisco IOS Software Releases* product bulletins on CCO. To locate these product bulletins on CCO, click **Login** and enter your user ID and password, and then follow this path:

Service & Support: Product Bulletins: Software

Under **Cisco IOS 11.3**, click **End of Sales and End of Engineering for Cisco IOS Software Releases 11.3 and 11.3 T (#847: 12/98)** or **Cisco IOS Software 11.3 NA EoS and EoE (#849:12/98)**.

Image Deferral, Cisco IOS Release 11.3(8)T

Cisco IOS Release 11.3(8)T was deferred to Release 11.3(8)T1 on all software images to incorporate corrections to the following caveats:

- CSCdk86294—The D channel is always in the shutdown state when non-facility associated signalling is configured.
- CSCdk80809—Enhanced Interior Gateway Routing Protocol (EIGRP) has difficulty converging on certain routes.

For more information on these caveats, refer to Bug Navigator II. Bug Navigator II is available at <http://www.cisco.com/support/bugtools>. On CCO, click this path:

Service & Support: Online Technical Support: Software Bug Toolkit: Bug Navigator II.

Enabling IPX Routing

Whenever IPX routing is enabled, the Token Ring interface resets.

Forwarding of Locally Sourced AppleTalk Packets

Cisco's implementation of AppleTalk does not forward packets with local-source and destination network addresses. This behavior does not conform to the definition of AppleTalk in Apple Computer's *Inside AppleTalk* publication. However, this behavior is designed to prevent any possible corruption of the AppleTalk Address Resolution Protocol (AARP) table in any AppleTalk node that collects MAC-addresses.

Missing Source-Route Bridging Commands

Due to a production problem, many source-route bridging commands were omitted from the printed version of the *Cisco IOS Software Command Summary (78-4746-XX)*. For documentation of all source-route bridging commands, see *Bridging and IBM Networking Command Reference (78-4743-XX)*. You can also obtain the most current documentation on CCO or on the Documentation CD-ROM.

New TACACS+ Attribute-Value Pair

A new authorization feature that allows you to separately configure and authorize Multilink PPP was added in Cisco IOS Release 11.3(1). This feature can cause MLP authorization to fail in TACACS+ servers that do not include the relevant authorization permissions in the configuration.

For TACACS+, add the following attribute-value (AV) pair for all users who are allowed to negotiate Multilink PPP:

```
service = ppp protocol = multilink {
```

40-bit Encryption Images are Unavailable in Release 11.3(1)

Cisco is conducting an internal review of the build and distribution processes associated with its 40-bit Cisco IOS cryptographic products. To provide seamless access to Cisco IOS 40-bit encryption capability, Cisco provides access to the most current 40-bit encryption images, beginning with Cisco IOS Release 11.2 (12), 11.2(12)P, and 11.3(2).

The following 40-bit encryption images are unavailable indefinitely:

- 11.2(1)–11.2(11.2)
- 11.2(2)P–11.2(11.1)P
- 11.2(1)F–11.2(4)F
- 11.3(1)

This review is not related to any new or previously unreported caveats. The information gathered in the review will be used to implement new automated development and order-processing applications.

Cisco IOS Syslog Failure

Certain versions of Cisco IOS software might fail or hang when they receive invalid User Datagram Protocol (UDP) packets sent to their syslog ports (port 514). At least one commonly-used Internet scanning tool generates packets, which can cause such problems. This fact has been published on public Internet mailing lists, which are widely read both by security professionals and by security crackers. This information should be considered in the public domain.

Attackers can cause Cisco IOS devices to repeatedly fail and reload, resulting in a completely disabled Cisco IOS device that will need to be reconfigured by its administrator. Some Cisco IOS devices have been observed to hang instead of failing when attacked. These devices do not recover until they are manually restarted by reset or power cycling. An administrator must personally visit an attacked, hung device to restart it, even if the attacker is no longer actively sending any traffic. Some devices have failed without providing stack traces; some devices might indicate that they were “restarted by power-on,” even when that is not the case.

Assume that any potential attacker is likely to know that existence of this problem and the ways to exploit it. An attacker can use tools available to the public on the Internet and does not need to write any software to exploit the vulnerability. Minimal skill is required and no special equipment is required.

Despite Cisco specifically inviting such reports, Cisco has received no actual reports of malicious exploitation of this problem.

This vulnerability notice was posted on Cisco’s World Wide Web site:

<http://www.cisco.com/warp/public/770/iosyslog-pub.shtml>

This information was also sent to the following e-mail and Usenet news recipients:

- cust-security-announce@cisco.com
- bugtraq@netspace.org
- first-teams@first.org (includes CERT/CC)
- first-info@first.org
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- nanog@merit.edu

Affected Devices and Software Versions

Vulnerable devices and software versions are specified in Table 1, *Affected and Repaired Software Versions*. Affected versions include Releases 11.3 AA, 11.3 DB, and all 12.0 versions (including 12.0 mainline, 12.0 S, 12.0 T, and any other regular released version whose number starts with 12.0), up to the repaired releases listed in Table 1. Cisco is correcting the problem in certain special releases and will correct it in future maintenance and interim releases. See Table 1, *Affected and Repaired Software Versions* for details. Cisco intends to provide fixes for all affected Cisco IOS variants.

No particular configuration is needed to make a Cisco IOS device vulnerable. It is possible to filter out attack traffic by using access lists. See the “Workarounds” section on page 12 for techniques. However, except at Internet firewalls, the appropriate filters are not common in customer configurations. Carefully evaluate your configuration before assuming that any filtering you have protects you against this attack.

The most commonly used or asked-about products are listed below. If you are unsure whether your device is running Cisco IOS software, log in to the device and issue the **show version** command. Cisco IOS software will identify itself simply as “IOS” or “Internetwork Operating System Software”. Other Cisco devices will not have the **show version** command, or they will identify themselves differently in their output. The most common Cisco devices that run Cisco IOS software include the following:

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 800,ubr900, 1000, 2500, 2600, 3000, 3600, 3800, 4000, 4500, 4700, AS5200, AS5300, AS5800, 6400, 7000, 7200 (including the ubr7200), 7500, and 12000 series
- Most recent versions of the LS1010 ATM switch
- Some versions of the Catalyst 2900XL LAN switch
- Cisco DistributedDirector

Affected software versions, which are relatively new, are not necessarily available on every device listed above. If you are not running Cisco IOS software, you are not affected by this problem.

The following Cisco devices are *not* affected:

- 700 dialup routers (750, 760, and 770 series)
- Catalyst 1900, 2800, 2900, 3000, and 5000 LAN switches are not affected, except for some versions of the Catalyst 2900XL. However, optional router modules running Cisco IOS software in switch backplanes, such as the RSM module for the Catalyst 5000 and 5500, are affected.
- WAN switching products in the IGX and BPX lines
- MGX (formerly known as the AXIS shelf)
- Host-based software

Important Notes

- Cisco PIX Firewall
- Cisco LocalDirector
- Cisco Cache Engine

This vulnerability has been assigned Cisco bug ID CSCdk77426.

Solution

Cisco offers free software updates to correct this vulnerability for all affected customers—regardless of their contract status. However, because this vulnerability information has been disseminated by third parties, Cisco has released this notice before updates are available for all software versions. Table 1 gives Cisco’s projected fix dates.

Make sure your hardware had adequate RAM to support the new software before installing it. The amount of RAM is seldom a problem when you upgrade within a major release (say, from 11.2(11)P to 11.2(17)P), but it is often a factor when you upgrade between major releases (say, from 11.2 P to 11.3 T).

Because fixes will be available for all affected releases, this vulnerability will rarely, if ever, require an upgrade to a new major release. Cisco recommends very careful planning for any upgrade between major releases. Make certain no known bugs will prevent the new software from working properly in your environment.

Further upgrade planning assistance is available on Cisco’s World Wide Web site at:

<http://www.cisco.com>

If you have service contracts you can obtain new software through your regular update channels (generally via Cisco’s World Wide Web site). You can upgrade to any software release, but you must remain within the boundaries of the feature sets you have purchased.

If you don’t have service contracts, you can upgrade to obtain only the bug fixes; free upgrades are restricted to the minimum upgrade required to resolve the defects. In general, you will be restricted to upgrading within a single row of Table 1, except when no upgrade within the same row is available in a timely manner. Obtain updates by contacting one of the following Cisco Technical Assistance Centers (TACs):

- +1 800 553 2447 (toll-free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- tac@cisco.com

Give the URL of this notice (<http://www.cisco.com/warp/public/770/iossyslog-pub.shtml>) as evidence for a free update. Non-contract customers must request free updates through the TAC. Please do not contact either “psirt@cisco.com” or “security-alert@cisco.com” for software updates.

Workarounds

You can work around this vulnerability by preventing any affected Cisco IOS device from receiving or processing UDP datagrams addressed to its port 514. This can be done either using packet filtering on surrounding devices, or by using input access list filtering on the affected Cisco IOS device itself.

If you use an input access list, apply that list to all interfaces to which attackers might be able to send datagrams. Interfaces include—not only physical LAN and WAN interfaces—but virtual subinterfaces of those physical interfaces, as well as virtual interfaces and interface templates corresponding to GRE, L2TP, L2F, and other tunneling protocols.

The input access list must block traffic destined for UDP port 514 at any of the Cisco IOS device's own IP addresses, as well as at any broadcast or multicast addresses on which the Cisco IOS device might be listening. Be sure to block both old-style "all-zeros" broadcasts and new-style "all-ones" broadcasts. It is not necessary to block traffic being forwarded to other hosts—only traffic actually addressed to the Cisco IOS device is of interest.

No single input access list works in all configurations. Know the effect of your access list in your specific configuration before activating it.

The following example shows a possible access list for a three-interface router, along with the configuration commands needed to apply the list. The example assumes input filtering is not needed, other than as a workaround for this problem:

```

! Deny all multicasts, and all unspecified-net broadcasts, to port 514
access-list 101 deny udp any 224.0.0.0 31.255.255.255 eq 514
! Deny old-style unspecified-net broadcasts
access-list 101 deny udp any host 0.0.0.0 eq 514
! Deny network-specific broadcasts. This example assumes that all of
! the local interfaces are on the class B network 172.16.0.0, subnetted
! everywhere with mask 255.255.255.0. This will differ from network
! to network. Note that we block both new-style and old-style broadcasts.
access-list 101 deny udp any 172.16.0.255 0.0.255.0 eq 514
access-list 101 deny udp any 172.16.0.0 0.0.255.0 eq 514
! Deny packets sent to the addresses of our own network interfaces.
access-list 101 deny udp any host 172.16.1.1 eq 514
access-list 101 deny udp any host 172.16.2.1 eq 514
access-list 101 deny udp any host 172.16.3.3 eq 514
! Permit all other traffic (default would be to deny)
access-list 101 permit ip any any

! Apply the access list to the input side of each interface
interface ethernet 0
ip address 172.16.1.1 255.255.255.0
ip access-group 101 in

interface ethernet 2
ip address 172.16.2.1 255.255.255.0
ip access-group 101 in

interface ethernet 3
ip address 172.16.3.3 255.255.255.0
ip access-group 101 in

```

Listing all possible addresses—especially all possible broadcast addresses—to which attack packets might be sent is complicated. If you do not need to forward any legitimate syslog traffic received on an interface, you can block all syslog traffic arriving on that interface. Remember that blocking will affect traffic routed through the Cisco IOS device as well as traffic destined to the device; if the Cisco IOS device is expected to forward syslog packets, you will have to do the detailed filtering. Because input access lists impact system performance, install them with caution—especially on systems running very near their capacity.

Software Versions and Fixes

Many Cisco software images have been or will be specially reissued to correct this vulnerability. For example, regular released version 12.0(2) is vulnerable, as are interim versions 12.0(2.1) through 12.0(2.3). The first fixed interim version of 12.0 mainline software is 12.0(2.4). However, a special release, 12.0(2a), contains only the fix for this vulnerability and does not include any other bug fixes from later 12.0 interim releases.

Important Notes

If you are running 12.0(2) and want to fix this problem without risking possible instability presented by installing the 12.0(2.4) interim release, you can upgrade to 12.0(2a). Release 12.0(2a) is a “code branch” from the 12.0(2) base, which will merge back into the 12.0 mainline at 12.0(2.4).

Special releases, like 12.0(2a), are one-time, spot fixes, and they will not be maintained. Thus, the upgrade path from 12.0(2a) is to 12.0(3).

Note All dates within this table are subject to change.

Table 1 Affected and Repaired Software Versions

Cisco IOS Major Release	Description	Special Fix ¹	First Fixed Interim Release ²	Fixed Maintenance Release ³
Unaffected Releases				
11.2 and earlier releases—all variants	Unaffected early releases (no syslog server)	Unaffected	Unaffected	Unaffected
11.3, 11.3 T, 11.3 DA, 11.3 MA, 11.3 NA, 11.3 WA, 11.3(2)XA	11.3 releases without syslog servers	Unaffected	Unaffected	Unaffected
Releases based on 11.3				
11.3 AA	11.3 early deployment for AS58xx	11.3(7)AA2, 8-JAN-1999 ⁴	11.3(7.2)AA	11.3(8)AA, 15-FEB-1999
11.3 DB	11.3 for Cisco NRP routing blade in Cisco 6400 xDSL DSLAM			11.3(7)DB2, 18-JAN-1999
Releases based on 12.0				
12.0	12.0 Mainline	12.0(2a), 8-JAN-1999	12.0(2.4)	12.0(3), 1-FEB-1999
12.0 T	12.0 new technology early deployment	12.0(2a)T1, 11-JAN-1999	12.0(2.4)T	12.0(3)T, 15-FEB-1999
12.0 S	ISP support; 7200, RSP, GSR		12.0(2.3)S, 27-DEC-1998	12.0(2)S ⁵ , 18-JAN-1999
12.0 DB	12.0 for Cisco 6400 universal access concentrator node switch processor (lab use)			12.0(2)DB, 18-JAN-1999
12.0(1)W	12.0 for Catalyst 8500 and LS1010	12.0(1)W5(5a) and 12.0(1a)W5(5b) (LS1010 platform only)	12.0(1)W5(5.15)	12.0(1)W5(6) (platform support for Catalyst 8540M will be in 12.0(1)W5(7))
12.0(0.6)W5	One-time early deployment for CH-OC12 module in Catalyst 8500 series switches	Unaffected; one-time release	Unaffected	Unaffected; To upgrade use 12.0(1)W5 releases.
12.0(1)XA3	Short-life release; merged to 12/0T at 12.0(2)T	Obsolete	Merged	Upgrade to 12.0(2a)T1 or to 12.0(3)T.
12.0(1)XB	Short-life release for Cisco 800 series; merged to 12.0 T and 12.0 (3)T	12.0(1)XB1	Merged	Upgrade to 12.0(3)T.

Table 1 Affected and Repaired Software Versions (continued)

Cisco IOS Major Release	Description	Special Fix ¹	First Fixed Interim Release ²	Fixed Maintenance Release ³
12.0(2)XC	Short-life release for new features in Cisco 2600, Cisco 3600, ubr7200, ubr900 series; merged to 12.0 T at 12.0(3)T	12.0(2)XC1, 7-JAN-1999	Merged	Upgrade to 12.0(3)T
12.0(2)XD	Short-life release for ISDN voice features; merged to 12.0 T at 12.0(3)T	12.0(2)XD1, 18-JAN-1999	Merged	Upgrade to 12.0(3)T
12.0(1)XE	Short-life release	12.0(2)XE, 18-JAN-1999	Merged	Upgrade to 12.0(3)T

- 1 A special fix is a one-time release that provides the most stable immediate upgrade path.
- 2 Interim releases are tested less rigorously than regular maintenance releases; interim releases can contain serious bugs.
- 3 Fixed maintenance releases are on a long-term upgrade path. Other long-term upgrade paths also exist.
- 4 All dates in this table are estimates and are subject to change.
- 5 This entry is not a misprint. The 12.0(2.3)S interim release is available before the 12.0(2)S regular release.

Deprecated MIBs

Old Cisco Management Information Bases (MIBs) will be replaced in a future release. OLD-CISCO-* MIBs are currently migrated into more scalable MIBs—without affecting existing Cisco IOS products or NMS applications. You can update from deprecated MIBs to the replacement MIBs as shown in the following table:

Table 2 Deprecated and Replacement MIBs

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	In Development
OLD-CISCO-DECNET-MIB	
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBS)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	

Caveats

Caveats describe unexpected behavior or defects in Cisco IOS software releases. This section contains open and resolved severity 1 and 2 caveats only for the current Cisco IOS maintenance release. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. All caveats in Release 11.3 and Release 11.3 T are also in Release 11.3(11)NA.

For information on caveats in Cisco IOS Release 11.3, refer to the “Important Notes and Caveats for Release 11.3” section in the cross-platform *Release Notes for Cisco IOS Release 11.3* document. For information on caveats in Cisco IOS Release 11.3 T, refer to the *Caveats for Cisco IOS Release 11.3 T* document. Both of these publications are on CCO and the Documentation CD-ROM.

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. From CCO, click **Login**, enter your user ID and password, and then click on this path: **Service & Support: Online Technical Support: Software Bug Toolkit**. You can also find Bug Navigator II at <http://www.cisco.com/support/bugtools>.

Caveats for Release 11.3(1) through 11.3(11)NA

This section describes possibly unexpected behavior by Release 11.3(11)NA. Only severity 1 and 2 caveats are included.

Miscellaneous

- CSCdm49454
Under certain timing conditions, the enabled command “cable ip-broadcast-echo” can cause a buffer leak. To work around this problem, do not enable the command “cable ip-broadcast-echo” or “cable ip-multicast-echo”.
- CSCdm51846
If an endpoint sends an Admission Request (ARQ) to the gatekeeper with more than one destination alias and the destination alias contains addresses that are not resolvable, the gatekeeper rejects the call when it reaches the first unresolved address and does not attempt to resolve the remaining addresses.

Caveats for Release 11.3(1) through 11.3(10)NA

This section describes possibly unexpected behavior by Release 11.3(10)NA. Only severity 1 and 2 caveats are included.

Access Server

- CSCdm21330
Configuring the MTU to be different from the default on a serial interface that was created by using a channelized group on an E1 4port controller generates the error “%DSX1-3-M32_MEM_ALLOC: Munich 32 channel memory allocation error” and puts the serial interface into an administrative shutdown state.

Interfaces and Bridging

- CSCdk67709

Multilink PPP interleaving causes a delay in outbound traffic on RSP platforms.

Miscellaneous

- CSCdk76257

In the downstream direction, (data) packets are not padded to the minimum length of 60 bytes. This might cause RUNT packets transmitted to the Ethernet behind a cable modem if the cable modem software does not pad to the minimum packet length. This used to be optional, but was changed recently in the specification and is now considered a bug. In Release 12.0 T, if CEF switching is enabled, packets shorter than the minimum permitted packet size are corrupted during transmission, and the modem receives packets with HCS errors. The workaround is to disable CEF switching.

- CSCdm08139

In Cisco IOS Release 11.3(8)T1, a Cisco router running 56 bit encryption and configured to run IPSec over a Frame-Relay Point-to-Point circuit fails. The packets from the source IP address are dropped at the router configured for IPSec.

- CSCdk85957

If the (Cable) MAC header received from cable modems has an odd length, Baseline Privacy is active, and flow switching or CEF switching is enabled, packets received from a cable interface and transmitted to another interface can become corrupted. If this problem occurs, several alignment errors are also reported.

- CSCdk87454

If BPI is active, or registration requests contain BPI fields, each registration request causes a memory leak of approximately 50 to 100 bytes. A workaround is to not enable BPI and to configure **cable qos permission modems**.

- CSCdk93483

If voice-traffic is process switched (such as when using RTP Header-Compression), the execution of certain EXEC commands on the router (such as **show running-config**) can have an adverse effect on the quality of voice-calls. The execution of the command competes with voice packets for CPU time.

- CSCdk94217

In some cases, the VCWare is not properly unbundled. The result is that no fax traffic passes. Re-load and unbundle the VCWare to resolve the problem.

- CSCdm06470

When HSRP is enabled on a cable interface, the system unexpectedly resets. The fix for this problem is to disable HSRP configuration on cable interfaces.

Note HSRP does not make sense on cable interfaces and must not be enabled.

- CSCdm08728

A Cisco router running Cisco IOS Release 11.3(6)T can unexpectedly restart if it is configured with **Crypto IPSEC** commands.

- CSCdm15557
If the timing adjustment is configured per upstream, Cisco CMTS can interop with a non-Broadcom base modem.
- CSCdm19926
If mismatched acls are in crypto maps, such as one side of the crypto connection having an acl-statement that the other side lacks, existing crypto connections can stop working after a period of time.
- CSCdm23824
Using any form of RSP turbo switching (optimum / flow / cef) on any type of Ethernet interface (10 Mbit / 100 Mbit / Gigabit) can cause packet errors in the MAC address fields of packets input from any interface sharing the same MEMD packet-free pools as the Ethernet interface.
There are two available workaround(s):
 - Disable all forms of RSP turbo switching by configuring **ip route-cache** on all interfaces.
 - Disable caching of MEMD using the command **test rsp cache memd uncached exec**, or by using the **memory cache-policy io uncached** configuration command.
- CSCdm24844
The wrong cause is identified when a voip call destination (IP) is unreachable. This can affect the re-routing capability of PABXs.
- CSCdm29993
Under rare conditions, the system reloads if a cable interface is shut down and subsequently re-enabled.
Three workarounds are available as follows:
 - Shut down all upstream channels first, then wait for a few seconds before shutting down the interface.
 - Shut down the interface connecting to the DHCP server, then shut down the cable interface.
 - Do not shut down the interface while modems are coming online.
- CSCdm49454
Under certain timing conditions, the enabled command “cable ip-broadcast-echo” can cause a buffer leak. To work around this problem, do not enable the command “cable ip-broadcast-echo” or “cable ip-multicast-echo”.
- CSCdm51846
If an endpoint sends an Admission Request (ARQ) to the gatekeeper with more than one destination alias and the destination alias contains addresses that are not resolvable, the gatekeeper rejects the call when it reaches the first unresolved address and does not attempt to resolve the remaining addresses.

Wide-Area Networking

- CSCdk68549
A router reloads when you use the command **no dialer remote-name [name]** while the router is actively trying to dial the named remote site. The workaround is to issue the command **shutdown** from config-if mode before issuing the command **no dialer remote-name [name]**.

- CSCdk76245

A Cisco Access Server that has been configured for AODI/X25/BAP/MPPP with the command “ppp multilink idle-link” causes a problem for NON-AODI clients using MPPP. A MPPP client when connected with more than one B-channel has the first channel in “receive” mode. The remainder belongs to same bundle in normal mode (send and receive).

Open Caveats for Release 11.3(8)NA

This section describes possibly unexpected behavior by Release 11.3(8)NA. Only severity 1 and 2 caveats are included.

Interfaces and Bridging

- CSCdk85541

An RSM running Cisco IOS Release 11.3(5)T, 11.3(6)T, or 11.3(7)T does not route an IP frame through a token-ring VLAN when transparent bridging is enabled on that VLAN. To work around this problem, configure IRB on the token-ring VLAN, and then route IP frames to the BVI.

Miscellaneous

- CSCdk29352

RADIUS attribute 61 is missing in Cisco IOS Release 11.3(4.4)T.

- CSCdk76257

In the downstream direction, (data) packets are not padded to the minimum length of 60 bytes. This might cause RUNT packets transmitted to the Ethernet behind a cable modem if the cable modem software does not pad to the minimum packet length. This used to be optional, but was changed recently in the specification and is now considered a caveat.

- CSCdk85957

If the (Cable) MAC header received from cable modems has an odd length, Baseline Privacy is active, and flow switching or CEF switching is enabled, packets received from a cable interface and transmitted to another interface can become corrupted. If this problem occurs, several alignment errors are also reported.

- CSCdk87454

If BPI is active, or registration requests contain BPI fields, each registration request causes a memory leak of approximately 50 to 100 bytes. A workaround is to not enable BPI and to configure **cable qos permission modems**.

Resolved Caveats for Release 11.3(8)NA

All the caveats listed in this section are resolved in Release 11.3(8)NA. Unless otherwise noted, this section describes only severity 1 and 2 caveats.

Basic System Services

- CSCdk59099
AAA connection accounting works for a single connection on the router, but with multiple connections. Start records are generated for all connections only the first disconnected call has a stop record generated; subsequent closed connections do not. All records have the same **Acct-session-id**. This problem exists in Release 11.3(2.4)T or later.

IBM Connectivity

- CSCdk30352
Cross-domain session drops might occur if **stun-tg** is configured on routers to connect two FEPs. When the session drop occurs, a `%SYS-2-BADSHARE: Bad refcount in datagram_done` might be reported by the router.

Miscellaneous

- CSCdk56804
The IP portion of an incoming call might not terminate correctly if the caller closes the connection. This situation is the result of rare timing conditions.
- CSCdk69483
Under a very rare circumstances the system can unexpectedly reset in **cmts_rx_interrupt**. This is caused by bad received data. This problem was only observed on MC11 cable line cards and only one time.
- CSCdk73672
An integrated access server can have modems which are unable to answer incoming calls under extremely high traffic load if the modems are set up to autoconfigure. The workaround is to re-enter the **modem autoconfigure type** command under the line.
- CSCdk78283
Before this fix, the CMTS might issue bad start allocation times and acknowledgment times in the upstream channel MAPs due to a bad counter mask value. This problem only occurs for the ASIC version of the cable line card.
- CSCdk92381
TCP/IP traffic that is routed between a TRISL subinterface and a Ethernet ISL subinterface might not be correctly fragmented. The workaround is to keep the TRISL subinterface MTU to 1500 or to move the TRISL subinterfaces to another hardware interface.

Novell IPX, XNS, and Apollo Domain

- CSCdk75750

Routing IPX between BRFs on a RSM running Release 11.3(7)T does not work when IPX route-cache is enabled on the BRF interfaces. A known workaround is to remove **ipx route-cache** from the BRF interfaces.

Wide-Area Networking

- CSCdk67735

VPDN does not support MS-CHAP. The workaround is to use CHAP or PAP.

Related Documentation

The following sections describe the publications related to Release 11.3(11)NA and how to access them on the World Wide Web and Cisco Documentation CD-ROM:

- Release-Specific Documents
- Hardware Documents
- Software Documents

Release-Specific Documents

Additional documentation for Cisco IOS Release 11.3(11)T is listed below.

- Release 11.3(11)NA release notes should be used in conjunction with the *Release Notes for Cisco IOS Release 11.3 T*. This document describes the release from which the current special release is derived and contains a list of Cisco 2500 series router and access server documentation. Release notes are located as follows:

— To reach the platform-specific release notes on CCO, click on this path:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Product Specific Release Notes for Cisco IOS Release 11.3: Cisco 2500 Series Routers

— To reach the platform-specific release notes on the documentation CD-ROM, click on this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Product Specific Release Notes for Cisco IOS Release 11.3: Cisco 2500 Series Routers

- Feature documentation is available on line only. New feature documentation supplements the Cisco IOS Release 11.3 T configuration guide and command reference publications; it includes configuration tasks and command reference pages.

To reach online feature documentation on CCO, click on this path: **Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release 11.3 NA Features**

- To reach product bulletins, field notices, and other release-specific documents on CCO, click on this path:

Service & Support: Technical Documents

- Caveats for Cisco IOS Release 11.3(11)NA are documented in these release notes. Because Cisco IOS Release 11.3(11)NA is based on Cisco IOS Release 11.3(11)T all caveats in Release 11.3(11)T are also in Release 11.3(11)NA. Caveats for Cisco IOS Release 11.3(11)T are documented in the *Caveats for Cisco IOS Release 11.3 T* document:

— To reach the Release 11.3(11)T caveats document from CCO, click on this path:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Caveats for Cisco IOS Release 11.3 T

— To reach the Release 11.3(11)T caveats document on the Documentation CD-ROM, click on this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Caveats for Cisco IOS Release 11.3 T

Note If you have an account with CCO, you can use Bug Navigator II to get additional information about caveats of any severity for any release. From CCO, log in and click on this path: **Service & Support: Online Technical Support: Software Bug Toolkit**. You can also find Bug Navigator II at <http://www.cisco.com/support/bugtools>.

Hardware Documents

Hardware documentation for the Cisco 2500 series routers ships with the Cisco 2500 series routers. To access these hardware documents on CCO, follow this path:

Service & Support: Documentation Home Page: Access Servers and Access Routers: Modular Access Routers: Cisco 2500 Series Modular Routers

or

Service & Support: Documentation Home Page: Access Servers and Access Routers: Fixed Configuration Access Routers: Cisco 2500 Series Routers

To access Cisco 2500 hardware documentation on the documentation CD-ROM, follow this path:

Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 2500 Series Modular Routers

or

Cisco Product Documentation: Access Servers and Access Routers: Fixed Configuration Access Routers: Cisco 2500 Series Routers

Software Documents

Cisco IOS software documentation consists of the Cisco IOS configuration guides and command references and also includes several supporting documents. These documents are shipped with the Cisco 2500 series routers in electronic form on the Documentation CD-ROM, unless you specifically ordered the printed version of the documents.

To access Cisco IOS software documents on CCO, follow this path:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3

To access software documentation on the documentation CD-ROM, follow this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3

Service and Support

For service and support for a product purchased from a reseller, contact the reseller. Resellers offer a wide variety of Cisco service and support programs, which are described in the section “Service and Support” in the information packet that shipped with your product.

Note If you purchased your product from a reseller, you can access CCO as a guest. CCO is the Cisco Systems primary real-time support channel. Your reseller offers programs that include direct access to CCO services.

For service and support for a product purchased directly from Cisco, use CCO.

Software Configuration Tips on the Cisco TAC Home Page

The following URL contains links to access helpful tips on configuring your Cisco products:

http://www.cisco.com/kobayashi/serv_tips.shtml

This URL is subject to change without notice. If it changes, point your web browser to <http://www.cisco.com/>, and follow this path: **Products & Technologies: Technical Tips**.

“Hot Tips” are popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC fax-on-demand service. To access fax-on-demand and receive documents at your fax machine from the USA, call 888-50-CISCO (888-502-4726). From other areas, call 415-596-4408.

The following sections are provided from the Technical Tips page:

- **Access Dial Cookbook**—Cisco Configuration Cookbooks offer easy-to-follow “recipes” for sample router configurations. The first cookbook in this new series contains network diagrams, sample configurations, and troubleshooting commands designed to help you set up and use various dial technologies on Cisco access routers.
- **Field Notices**—Designed to provide notification of any critical issues regarding Cisco products. These include problem descriptions, safety or security issues, and hardware defects.
- **Hardware**—Technical Tips related to specific hardware platforms.
- **Internetworking Features**—Tips on using and deploying Cisco IOS software features and services.
- **Sample Configurations**—Actual configuration examples complete with topology and annotations.
- **Software Products**—MultiNet & Cisco Suite 100, Network Management, Cisco IOS Software Bulletins, and CiscoPro Configurations.
- **Special Collections**—Other Helpful Documents, Frequently Asked Questions, Security Advisories, References & RFCs, Case Studies, and the CiscoPro Documentation CD-ROM.

Cisco Connection Online

Cisco Connection Online (CCO) is the Cisco Systems primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: [cco.cisco.com](telnet://cco.cisco.com)
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact the Cisco Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Access Registrar, AccessPath, Any to Any, AtmDirector, CCDA, CCDE, CDDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Technologies logo, ConnectWay, ControlStream, Fast Step, FireRunner, GigaStack, IGX, JumpStart, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, New World, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, RouteStream, Secure Script, ServiceWay, SlideCast, SMARTnet, StreamView, *The Cell*, TrafficDirector, TransPath, ViewRunner, VirtualStream, VisionWay, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and Asist, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9906R)

Copyright © 1999, Cisco Systems, Inc.
All rights reserved.

